UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,862	02/25/2004	Sergey Shokhor	1361008-2019/10.100	3678

38878   7590   05/11/2011
F5 Networks, Inc.
c/o Frommer Lawrence & Haug LLP.
745 Fifth Avenue
NEW YORK, NY 10151

EXAMINER
KEEHN, RICHARD G

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
05/11/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/786,862	SHOKHOR ET AL.
Office Action Summary	Examiner	Art Unit
	RICHARD G. KEEHN	2456

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _13 January 2011_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-33_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-33_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-33 have been examined and are pending.

2.   Claim 34 was previously cancelled.

3.   No new claims are presented.

Continued Examination Under 37 CFR 1.114

4.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

01/13/2011 has been entered.

Response to Arguments

5.   Applicant's arguments filed 1/13/2011 have been fully considered but they are

not persuasive.

    a.   On pages 10, 11 and the first two paragraphs of 12, Applicant argues that

the limitations "receiving from the downloaded component the configuration of

the client device based on the inspection; in response to the received request,

applying, using the apparatus, a dynamic policy for the access based, in part, on

the received configuration and the requested resource" are not disclosed.

Applicant bases the argument on the combination of Wright and Knouse alone,

but Shah was also used in combination to teach that which Applicant alleges in

not disclosed. Applicant later on page 12 through the first paragraph of 13 states

that Shah fails to cure deficiencies in that Shah does not disclose the recited

apparatus applying a restriction to the client device. Looking at the rejection,

Shah was not relied upon for this disclosure, but rather Wright. The combination

of all three references was used to disclose the claim.

b.   Applicant's argument against the rejection of the dependent claims is

based on independent claim arguments alone, except for *allegedly amended*

Claim 9 which is presented as "(Previously Presented)". Nonetheless, Claim 9's

limitation is met because Wright, the primary reference, discloses preventing

access to hackers. Doing so prohibits file saves and reads.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

6.   Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over US

7,308,703 B2 (Wright et al.), and further in view of US 7,185,364 B2 (Knouse et al.).

As to Claim 32, Wright et al. anticipate a method implemented at a server device

for managing access to a resource over a network, comprising:

Receiving a request for access to the resource from a client device (Wright et al.

disclose reception of client request – Figure 10A, elements 1014 and 1024);

determining a level of security software enabled on the client device (Wright et al.

disclose determining a client's security software status as active or inactive and basing

restrictions to client access based on the client's security status – Column 2, lines 17-

64; In addition, column 2, lines 60-64 disclose that security features of the

communication session between the mobile device and another computer are

determined. In other words, to check the session's security features, one *or both*

communicating party's security configuration is checked.)

including what antivirus software is active on the client device (Wright et al.

disclose policy based on anti-virus software status - Column 18. lines 35-39)

and whether a hacker tool is enabled on the client device (Wright et al. Column

20, lines 35-42 disclose that the security software can be a hacker tool VPN);

applying a dynamic policy to the access based, in part, on the determined level of

security software enabled (Wright et al. disclose determining a client's security software

status as active or inactive and basing restrictions to client access based on the client's

security status – Column 2, lines 17-64; and both of the communicating devices are

checked for security features because the communication session is analyzed between

the mobile device and another computer - 2:60-64, 7:11-14, and 7:28-36); and

applying a restriction to the client device for access by the client device to the

requested resource, the restriction based on the applied dynamic policy (Wright et al.

disclose determining a client's security software status as active or inactive and basing

restrictions to client access based on the client's security status – Column 2, lines 17-

64; and both of the communicating devices are checked for security features because

the communication session is analyzed between the mobile device and another

computer - 2:60-64, 7:11-14, and 7:28-36).

Wright et al. disclose that the communication session between two devices is

examined for security status, and the dynamic policy application, however they are not

explicit on using the server device to apply communication restrictions. However,

Knouse et al. disclose

at the server device (Knouse et al. disclose using the server device to apply a

policy in response to t user request for resource access based on the requestor's

configuration and the nature of the resources requested - 8:32-66),

using the server device (Knouse et al. disclose using the server device to apply a

policy in response to t user request for resource access based on the requestor's

configuration and the nature of the resources requested - 8:32-66); and

in response to the received request (Knouse et al. disclose using the server

device to apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66); and

and the requested resource (Knouse et al. disclose using the server device to

apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to combine using the server device to apply communication

restrictions; and in response to the received request; and the requested resource taught

by Knouse et al., with applying the dynamic policy taught by Wright et al., in order to

customize responses to individual users – (Knouse et al. - 8:32-66).

7.   **Claims 1, 2, 4-11, 13-18 and 20-31 are rejected under 35 U.S.C. 103(a) as**

being unpatentable over US 7,308,703 B2 (Wright et al.), and further in view of US

7,430,524 B2 (Shah et al.), and US 7,185,364 B2 (Knouse et al.).

As to Claims 1, 10, 22, 28 and 31, Wright et al. disclose an apparatus, method

implemented at a network device, a network appliance and a computer readable

storage medium that includes data and instructions, wherein the execution of the

instructions on a computing device provides, and an apparatus, respectively, for

managing access to a resource over a network, comprising:

a receiver that receives a request for access to the resource from a client

device (Wright et al. disclose reception of client request – Column 15, lines 62-63); and

a policy manager, coupled to the receiver, that is performs actions,

including (Wright et al. disclose the policy module – Column 15, lines 40-42):

including determining whether client security software other than a virtual

sandbox is active on the client device (Wright et al. disclose determining a

client's security software status as active or inactive and basing restrictions to

client access based on the client's security status – Column 2, lines 17-64);

the configuration of the client device based on the inspection (Wright et al.

disclose determining a client's security software status as active or inactive and

basing restrictions to client access based on the client's security status – Column
2, lines 17-64);

applying a dynamic policy for the access based, in part, on the received
configuration (Wright et al. disclose determining a client's security software status
as active or inactive and basing restrictions to client access based on the client's
security status – Column 2, lines 17-64); and

applying a restriction to the client device for access by the client device to
the requested resource, the restriction based on the applied dynamic policy
(Wright et al. disclose determining a client's security software status as active or
inactive and basing restrictions to client access based on the client's security
status – Column 2, lines 17-64);

and whether a hacker tool is enabled on the client device (**CLAIM 31
Only**) (Wright et al. Column 20, lines 35-42 disclose that the security software
can be a hacker tool VPN).

Wright et al. disclose that the communication session between two devices is
examined for security status, and the dynamic policy application, however they are not
explicit on using the apparatus to apply communication restrictions. However, Knouse et
al. disclose

using the apparatus (Knouse et al. disclose using the server device to apply a
policy in response to t user request for resource access based on the requestor's
configuration and the nature of the resources requested - 8:32-66); and

from the client device (Knouse et al. disclose using the server device to apply a

policy in response to t user request for resource access based on the requestor's

configuration and the nature of the resources requested - 8:32-66);

in response to the received request (Knouse et al. disclose using the server

device to apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66); and

and the requested resource (Knouse et al. disclose using the server device to

apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66).

The motivation and obviousness arguments for Knouse et al. are the

same as in Claim 32.

The combination of Wright et al. and Knouse et al. does not disclose

downloading a component onto the client device, wherein the downloaded

component inspects the client device to detect a configuration of the client device

and receiving from the downloaded component, but Shah et al. disclose

downloading a component onto the client device, wherein the downloaded

component inspects the client device to detect a configuration of the client device

(Shah et al. – Column 76, lines 9-25 disclose downloading an agent onto a client

device to inspect the client device to determine the client device's configuration,

and reporting said configuration back to the server that sent the agent); and

receiving from the downloaded component (Shah et al. – Column 76, lines

9-25 disclose downloading an agent onto a client device to inspect the client

device to determine the client device's configuration, and reporting said configuration back to the server that sent the agent).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine sending an agent to determine a client's configuration and reporting back to the sender taught by Shah et al. with determining the client configuration taught by the combination of Wright et al. and Knouse et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to determine information regarding a plurality of client devices for system modeling (Shah et al. – Column 76, lines 40-51).

As to Claim 2, the combination of Wright et al., Knouse et al. and Shah et al. discloses the apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to not download the component, then receiving the configuration of the client device through a browser residing on the client device (Shah et al. disclose the server capable of determining client's configuration via a plug and play interface which those of ordinary skill in the art would know to include plug and play browsers, as an alternative to the downloadable component determining the configuration and sending it back to the server – Column 76, lines 15-22).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 4, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1, wherein determining the configuration of the client

device further comprises

determining information associated with the connection between the client device

and the resource (Wright et al. disclose determining information associated with the

communication session between the mobile device and another computer – Column 3,

lines 4-8).

As to Claim 5, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1, wherein inspecting the client device to detect a

configuration further comprises

detecting if security software is installed on the client device and if security

software is installed, inspecting the security software to detect if the security software is

active or disabled (Wright et al. disclose determining a client's security software status

as active or inactive and basing restrictions to client access based on the client's

security status – Column 2, lines 17-64).

As to Claim 6, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1, wherein applying the restriction further comprises

employing a virtual sandbox that is configured based on the applied dynamic

policy (Wright et al. Column 20, lines 35-42 disclose that the security software can be a

hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 7, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1,

wherein the restriction includes at least one downloadable component (Wright et

al. disclose determining a client's security software status as active or inactive and

basing restrictions to client access based on the client's security status – Column 2,

lines 17-64).

As to Claim 8, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1,

wherein the restriction intercepts a communication between the client device and

the apparatus (Wright et al. discloses the interception of files as a restriction – Column

7, lines 59-67).

As to Claim 9, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the apparatus of claim 1, wherein applying the restriction further comprises

performing at least one of inhibiting a file save, and inhibiting a file print (Wright

et al. discloses inhibiting a file save by preventing write access to hackers – 20:35-42).

As to Claim 11, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, further comprising

in response to receiving the request for access to the resource, transmitting a

downloadable component to the client device (Wright et al. disclose determining a

client's security software status as active or inactive and basing restrictions to client

access based on the client's security status – Column 2, lines 17-64).

As to Claim 13, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating at least one of one level of trust associated with

the client device, a type of encryption enabled on the client device, a type of antivirus

enabled on the client device, a security feature enabled on the client device, a browser

type, an operating system configuration, a security certificate, and if a hacker tool is

enabled on the client device (Wright et al. disclose determining a client's security

software status as active or inactive and basing restrictions to client access based on

the client's security status – Column 2, lines 17-64; Wright et al. Column 20, lines 35-42

disclose that the security software can be a hacker tool VPN).

As to Claim 14, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating a level of trust of the client device (Wright et al

disclose the trust level determination – Column 18, lines 19-23).

As to Claim 15, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating a characteristic of an enabled security application

enabled (Wright et al disclose the trust level determination – Column 18, lines 19-23).

As to Claim 16, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein applying the restriction further comprises

downloading a component to the client device (Wright et al. disclose determining

a client's security software status as active or inactive and basing restrictions to client

access based on the client's security status – Column 2, lines 17-64).

As to Claim 17, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein applying the restriction further comprises

configuring a virtual sandbox to intercept a communication between the client

device and the resource (Wright et al. discloses the interception of files as a restriction –

Column 7, lines 59-67; Wright et al. Column 20, lines 35-42 disclose that the security

software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 18, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 17, wherein intercepting the communication further

comprises

blocking a download of at least one file to the client device (Wright et al.

discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 20, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein applying the dynamic policy further

comprises

determining at least one of a connector, and an adaptor to enable the access to

the resource (Wright et al. disclose the determination of network adapter - Column 7,

lines 26-37).

As to Claim 21, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the method of claim 10, wherein applying the dynamic policy further

comprises

restricting the access to the resource (Wright et al. discloses the interception of

files as a restriction – Column 7, lines 59-67).

As to Claim 23, the combination of Wright et al., Knouse et al. and Shah et al. discloses the network appliance of claim 22, wherein the processor is configured to perform further actions, comprising:

in response to receiving the request for access to the resource, receiving additional information about the configuration of the client device through a query with a browser residing on the client device (Shah et al. – Column 76, lines 15-22 disclose the server capable of determining client's configuration via a plug and play interface which those of ordinary skill in the art would know to include plug and play browsers, as an alternative to the downloadable component determining the configuration and sending it back to the server).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 24, the combination of Wright et al., Knouse et al. and Shah et al. discloses the network appliance of claim 22, wherein applying the restriction further comprises

employing a virtual sandbox that is configured based on the applied dynamic policy (Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 25, the combination of Wright et al., Knouse et al. and Shah et al. discloses the network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is not configured to receive a downloadable component,

receiving information about the configuration of the client device through a browser

application residing within the client device (Shah et al. disclose the server capable of

determining client's configuration via a plug and play interface which those of ordinary

skill in the art would know to include plug and play browsers, as an alternative to the

downloadable component determining the configuration and sending it back to the

server – Column 76, lines 15-22).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 26, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the network appliance of claim 22, wherein applying the dynamic policy further

comprises:

if the client device is configured to restricting a download of a component,

restricting access to the resource (Wright et al. disclose determining a client's security

software status as active or inactive and basing restrictions to client access based on

the client's security status – Column 2, lines 17-64).

As to Claim 27, the combination of Wright et al., Knouse et al. and Shah et al.

discloses the network appliance of claim 22, wherein applying the restriction further

comprises:

if the client device is configured to restrict a download of a component,

intercepting a communication between the client device and the requested resource to

perform at least one of preventing an access to file, and restricting an action (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 29, the combination of Wright et al., Knouse et al. and Shah et al. discloses the computer readable storage medium of claim 28, wherein applying the restriction further comprises

configuring a Virtual sandbox to intercept a communication between the client device and the resource (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67; Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 30, the combination of Wright et al., Knouse et al. and Shah et al. discloses the computer readable storage medium of claim 28, wherein applying the restriction further comprises

blocking a download of at least one file to the client device (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

8.   **Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Wright et al., Knouse et al. and Shah et al. as applied to claim 10 above, and further in view of US 7,200,272 B2 (Ishikawa).**

As to Claim 19, the combination of Wright et al., Knouse et al. and Shah et al. discloses the method of claim 10.

The combination of Wright et al., Knouse et al. and Shah et al. does not disclose if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command, but Ishikawa discloses, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command (Ishikawa – Column 5, lines 2-12 disclose the client's cache manager deleting the user's cache as part of a cleanup).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command taught by Ishikawa, with applying a restriction to the access for the requested resource based on the applied dynamic policy taught by the combination of Wright et al., Knouse et al. and Shah et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to avoid system resources from sitting at their maximum limit, thus freeing up resources for other applications to use (Ishikawa - Column 5, lines 8-12).

9.   Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Wright et al., Knouse et al. and Shah et al., and further in view of US 2002/0111852 A1 (Levine).

As to Claim 3, the combination of Wright et al., Knouse et al. and Shah et al. discloses the apparatus of claim 1.

The combination of Wright et al., Knouse et al. and Shah et al. does not disclose wherein the received configuration indicates whether the client device is operating as a kiosk, but Levine discloses

wherein the received configuration indicates whether the client device is operating as a kiosk (Levine – Page 2, ¶ [0022] discloses determining the type of client device and whether it's a cell phone, kiosk, PDA, laptop, desk computer, terminal or any other access device).

The motivation and obviousness arguments are similar to that of Claim 33.

As to Claim 12, the combination of Wright et al., Knouse et al. and Shah et al. discloses the method of claim 10, wherein receiving the configuration further comprises.

The combination of Wright et al., Knouse et al. and Shah et al. does not disclose receiving information indicating whether the client device is a laptop, personal computer, kiosk, or a mobile device, but Levine discloses

receiving information indicating whether the client device is a laptop, personal

computer, kiosk, or a mobile device (Levine – Page 2, ¶ [0022] discloses determining

the type of client device and whether it's a cell phone, kiosk, PDA, laptop, desk

computer, terminal or any other access device).

The motivation and obviousness arguments are similar to that of Claim 33.

10.   Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over US

7,308,703 B2 (Wright et al.), and further in view of US 2002/0111852 A1 (Levine),

and US 7,185,364 B2 (Knouse et al.).

As to Claim 33, Wright et al. disclose a method implemented at a network

appliance for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Wright et al.

disclose reception of client request – Column 15, lines 62-63);

determining whether client computing security software is active on the client

device or whether a hacker tool is enabled on the client device (Wright et al. disclose

determining a client's security software status as active or inactive and basing

restrictions to client access based on the client's security status – Column 2, lines 17-

64; Wright et al. Column 20, lines 35-42 disclose that the security software can be a

hacker tool VPN); and

applying a restriction to the client device for access by the client device to the

requested resource, the restriction based on the determined configuration of the client

device (Wright et al. disclose determining a client's security software status as active or

inactive and basing restrictions to client access based on the client's security status –

Column 2, lines 17-64, Figure 10A, elements 1024-1034).

Wright et al. disclose that the communication session between two devices is

examined for security status, and the dynamic policy application, however they are not

explicit on using the server device to apply communication restrictions. However,

Knouse et al. disclose

using the network appliance (Knouse et al. disclose using the server device to

apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66); and

in response to the received request (Knouse et al. disclose using the server

device to apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66); and

and the requested resource (Knouse et al. disclose using the server device to

apply a policy in response to t user request for resource access based on the

requestor's configuration and the nature of the resources requested - 8:32-66).

The motivation and obviousness arguments for Knouse et al. are the same as in

Claim 32.

The combination of Wright et al. and Knouse et al. does not explicitly disclose

determining if the client device is configured as a kiosk or a mobile device, but Levine

discloses

determining if the client device is configured as a kiosk or a mobile device

(Levine – Page 2, ¶ [0022] discloses determining the type of client device and whether

it's a cell phone, kiosk, PDA, laptop, desk computer, terminal or any other access

device).

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to combine determining if the client device is configured as a kiosk

or a mobile device taught by Levine, with determining client configuration taught by the

combination of Wright et al. and Knouse et al., in order to personalize content delivery

(Levine – Page 2, ¶ [0015]).

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. These were presented in a prior Office action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to RICHARD G. KEEHN whose telephone number is

(571)270-5007. The examiner can normally be reached on Monday through Thursday,

9am - 8pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rupal D. Dharia/
Supervisory Patent Examiner, Art
Unit 2456

RGK